基于区块链的分布式激励机制研究

何云华[1]，刘昭阳[1]，胡 堰[3]，李 红[2]，孙利民[2]，肖 珂[1]

(1. 北方工业大学 计算机学院，北京 100144; 2. 中国科学院信息工程研究所 物联网安全北京市重点实验室，北京 100093; 3. 北京科技大学 计算机与通信工程学院，北京 100091)

摘 要：激励机制广泛应用于群智感知、P2P 视频点播、机会网络等场景中，是提升信息网络服务质量与效率的关键。现有的激励机制通常依赖于类似银行的可信中心，但可信中心因其管控不透明、易受攻击等特征而存在系统信任缺失和隐私泄露问题。基于区块链的激励机制可作为上述问题的解决方案，区块链具有去中心化、开放性、不可窜改、匿名性等特征，可在互不了解的多方间建立了可靠的信任关系，而且基于区块链的密码货币获得现实世界广泛的关注和认可。首先介绍区块链技术及密码货币差异，然后总结基于区块链的激励机制研究现状，包括激励机制交易形式、激励机制分类，激励机制评价标准。最后对现有激励机制研究总结和展望。

关键词：激励机制；区块链；密码货币；支付策略；激励效果

中图分类号：TP309.7　　doi: 10.19734/j.issn.1001-3695.2020.03.0029

Research on distributed incentive mechanism based on blockchain

He Yunhua[1], Liu Zhaoyang[1], Hu Yan[3], Li Hong[2], Sun Limin[2], Xiao Ke[1]

(1. *School of Information Science & Technology*, *North China University of Technology*, *Beijing* 100144, *China*; 2. *Beijing Key Laboratory IoT Information Security Technology*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*; 3. *School of Computer & Communication Engineering*, *University of Science & Technology Beijing*, *Beijing* 100091, *China*)

Abstract: Incentive mechanism is the key to improve the quality and efficiency of information network service, and is widely used in crowdsensing applications, P2P VoD streaming, opportunistic networks and so on. The existing incentive mechanisms usually rely on trusted centers like banks, but the trusted centers may have the problems of a lack of trust and privacy leakage due to the systems’ vulnerability and the trusted centers’ opacity. The incentive mechanism based on blockchain can be used as a solution to the above problems. For one reason, blockchain is decentralized, open, tamper-resistant and semi-anonymity, and it can establish a trust among multiple parties who do not know each other. Moreover, the cryptocurrency based on blockchain has been paid more and more attentions and has been gradually accepted by people. This paper firstly summarizes the blockchain technology and the differences of cryptocurrencies, then presents the research stratus of incentive mechanisms based on blockchain including the incentive mechanism transactions, the common incentive mechanisms and the evaluation of the incentive mechanisms. Finally, it summarize and looks forward to the research of the existing incentive mechanism.

Key words: incentive mechanism; block Chain; cryptocurrency; payment policy; incentive effect

0 引言

在信息网络中，激励机制得到了广泛的应用，如在智能交通系统中电子货币被用于激励用户分享交通实时信息[1]，在网易云音乐中用户等级制度被用于激励用户提升使用软件活跃性，在共享单车系统中用户抽奖机会被用于激励用户上传损坏车辆信息，在博客、论坛上奖励积分被用于激励用户发表文章、帖子等，激励机制还可应用于延迟容忍网络[2]、无线频谱分配[3]等方向。激励机制是通过设计合理的报酬形式，以一定的行为规范和奖惩措施，来激励用户规范行为，如抑制节点自私、促进节点协作、提升节点贡献等，是提高服务质量、效率的有效保障。

电子货币作为信息网络普遍采用的激励方式[4~7]，其发行大多依赖于权威机构，如银行、政府部门等可信中心，然而这种方式存在着诸多问题。可信中心对于整个系统拥有着绝对的控制权，包括电子货币的发行和交易数据的掌握，可信中心发行、记账、维护过程不透明以及其不规范操作、防护手段不完备等行为造成了信任缺失问题，一旦被恶意攻击者攻击，将影响整个系统运行。现实中可信中心遭到攻击、数据泄露事件频繁发生，如 2017 年 11 月五角大楼违规操作致 18 亿用户个人信息泄露，2017 年 11 月黑客攻击 Uber 获取 5000 万用户信息[8],2016 年 4 月土耳其数据库因存在安全漏洞致 5000 万用户信息遭泄露[9]。

区块链技术可被用于解决信任缺失问题。区块链具有可追溯、无须信任、去中心化、不可窜改、匿名性等特性，使用共识机制、非对称加密、块链结构等技术，可在互不了解的多方间建立可靠的信任关系，实现节点间的信息交互。基于区块链的分布式激励方式可以增强系统的安全性和容灾性。

现在分布式激励机制设计基本都是依据应用场景进行设计，如迅雷推出的基于区块链的“玩客币”用于激励用户上传的闲置资源转换为共享计算服务，Wang 等人[10]根据群智感知应用提出了一种基于区块链的激励机制。已有文献更倾向于依据场景进行激励机制设计，本文则结合激励机制中在不同场景下的设计进行差异分析，在此基础上介绍基于区块链的激励机制研究进展包括方式、分类、评价。本文第二节介绍了区块链技术、分析了密码货币的差异；第三节讨论基于区块链的激励机制，包括具体的激励交易形式、激励机制分类介绍；第四节阐述了激励机制的评价标准；第五节对现

收稿日期：2020-03-02；**修回日期：**2020-06-01

作者简介：何云华，男，博士，主要研究方向为区块链技术(sadwewresfdd517@163.com).

有激励机制工作进行了总结，以及对未来基于区块链技术的激励机制的展望。

1　区块链技术及密码货币

区块链作为比特币的底层技术，由中本聪在《Bitcoin: A Peer-to-Peer Electronic Cash System》白皮书中首次提出。首创区块链的比特币使用了分布式时间戳技术来解决电子支付中的"重复花费"问题，其因去中心化、开放性、独立性、安全性、一定匿名性等特性而得到广泛关注、应用。在区块链网络中，通过 PoW 共识算法、非对称加密、哈希算法等技术来保证区块链的安全、可靠。区块链中的安全性依赖于大量矿工节点的参与，区块链本身的激励机制通过激励遵守规则参与记账的节点，并且惩罚不遵守规则的节点，使整个系统朝着良性循环的方向发展。本文更关注于利用基于区块链的密码货币来设计激励机制，以提升相关网络应用与系统的安全性。

基于区块链的密码货币作为使用区块链和密码学原理来确保交易安全创造的电子货币，其不依靠货币机构发行，是一种 P2P 形式的加密数字货币，具有去中心化、交易安全、健壮性等特性。近年来随着区块链技术的广泛应用[11~13, 15]，密码货币的种类也越来越多。现有的大部分密码货币如 Bitcoin、ETH、Litecoin、XRP、Zerocoin 等具有价值稳定、流通性好的基本特征，也存在差异化的特征，如表 1 所示。

表 1　密码货币对比分析

Tab. 1　Comparative analysis of cryptocurrency

密码货币	共识协议	生成区块速度	主要特点
Bitcoin	PoW	10 分钟	首创加密货币，认可度高
ETH	PoW/PoS	15 秒	智能合约功能，支持建立应用，易于实现定价策略
Litecoin	Scrypt 工作量证明	2.5 分钟	Scrypt 算法比 SHA256 更安全，更有利于防止 51%攻击
XRP	RPCA	3 秒	共识节点为可信节点，低成本，可拓展性高，安全性差
Zerocoin	零币协议	2.5 分钟	零币协议采用零知识证明保护用户隐私

Bitcoin 是由中本聪[14]提出的基于区块链技术的加密货币。首创区块链的 Bitcoin 使用了分布式时间戳技术来解决电子支付中的"重复花费"问题，其因去中心化、开放性、独立性、安全性、一定匿名性等特性而得到广泛关注、应用。在 Bitcoin 网络中，维护系统需要较高的成本，计算消耗了大量电力。其次，Bitcoin 交易到账慢，Bitcoin 网络约 10 分钟产生一个新的区块，交易确认时间至少需要一小时。Bitcoin 不能保证用户的完全匿名性，真实身份信息可能会因关联信息追踪到。Bitcoin 的交易语法只支持转账，当直接作为激励手段时，可能出现激励者或被激励者的抵赖行为，因此作为激励方式时，应扩充 Bitcoin 的交易语法，使其支持功能性转账，来确保激励机制的正常运作。

ETH 是基于 Ethereum 的数字代币，通过 Ethereum 可编程智能合约及开源系统，实现高灵活性 ETH 交易。Ethereum 基于区块链 2.0 基础上使用智能合约功能，智能合约赋予了区块链高灵活度的拓展应用功能，可控制区块链上的数字资产进行复杂操作，智能合约具有可自动执行、不可窜改、可追踪的特性，可写入交易双方的合约要求、相应规定要求等，易于实现激励机制中的定价策略。ETH 采用了 PoS 共识机制激励获取 ETH 奖励，交易效率达到 15 秒一个区块，也降低了处理数据成本。ETH 无固定总量，发行量上限为每年 1800 万。

Litecoin 相比于 Bitcoin 在工作量证明机制算法、总量上限和区块生成速度上作出了改进。Litecoin 在工作量证明机制中使用 Scrypt 算法取代 SHA-256 算法，将在 Bitcoin 只由 CPU 处理速度决定算力的情形替代为由 CPU 和内存共同决定，这一改变使得运算能力难以集中，不能像 Bitcoin 那样形成大量的矿场矿池，而挖矿的矿工更加分散，因此也就更利于防止 51%攻击。Litecoin 网络适用于对安全性有较高要求的激励机制。Litecoin 固定总量由 Bitcoin 的 2100 万提升至 8400 万，区块速度为 2.5 分钟一个，完成一笔交易的时间约为 20 分钟。目前 Litecoin 是除了比特币以外关注度、认可度最高的数字货币。

XRP 基于 Ripple 网络实现交易，该网络支持全球不同分类账本和网络之间即时、低成本的国际支付，交易费用几乎为零。XRP 是 Ripple 网络中的基础货币，总数量为 1000 亿个，随着交易的增多而减少，每发起一笔转账就需要支付微量的瑞波币给到网络并销毁。基于 Ripple 协议中的共识机制与验证机制，XRP 相比于 Bitcoin 的交易数据打包和记录确认速度更快。其共识机制为协议共识，将网络中的节点分为普通节点和验证节点，交易的验证和确定只需要验证节点的投票，因此 XRP 不需要挖矿。激励机制场景中需要交易延时低的交易系统以及高效率的支付手段。因此当需要考虑转账成本、效率、跨境汇款等问题时，XRP 可以确保这些问题的解决。

Zerocoin 作为比特币的一种分支保留了其原有的模式，其总量为 2100 万，工作量证明机制使用 Equihash 算法，其更加依赖于 GPU。相较于 Bitcoin 来说，Zcash 仍属于小众数字货币，但 Zerocin 解决了比特币匿名程度不够的问题。Zerocoin 分为两种资金，透明资金和私有资金。透明资金与比特币相似，Zerocoin 提供完全公开的地址，交易记录可查。私有资金以保护用户隐私为目的，使用 zk-SNARKS 加密技术实现匿名，使交易记录和金额彻底隐藏，其交易记录不公开，通过私钥查看交易记录，解决了相对于 Bitcoin 中存在的"伪匿名"问题。因此 Zerocoin 作为激励方式时，它的交易规则可以隐藏激励机制中交易双方的身份信息及交易记录，适用于需要更完善的隐私保护的场景。

2　基于区块链的激励机制

激励机制是指运用多种激励方法促使组织者、参与者高效率的协同合作、完成目的，达到利益最大化。基于区块链的激励机制将基于区块链的密码货币作为激励机制的激励方式，具有去中心化、交易安全、健壮性等特性。其中组织者、参与者可在互不信任、无第三方监管的情况下协同合作，使用密码货币作为任务的报酬，依据不同的密码货币自身属性为交易提供了隐私保护、低延时、低成本，通过微支付通道、线下交易等技术保证交易的高吞吐、可信安全。

激励机制的设计应该考虑不同的应用场景。不同的应用场景下，其角色关系及利益关系不同，导致交易验证、报酬流向的设置不同。例如，在路况众包感知系统的激励机制中[16]，系统包含任务发起者、参与者和验证者三个角色，由任务发起者发起一个地理位置的交通状况查询请求并将报酬交付给服务器，该地点附近的参与者通过协作的方式进行感知任务，验证者验证参与者任务后，与参与者按相应比例获取发起者交付给服务器的报酬，从而提高用户安全交易和分享信息的积极性。视频点播应用基于 P2P 网络的流媒体分发激励机制中[17]，包括点播服务器和贡献带宽节点两个角色，点播服务器给高贡献带宽的节点较好的视频服务质量，隔离低贡献率的节点，以达到避免 P2P 网络的搭便车问题。在延迟容忍网络缓存、转发文件的激励机制中[18]，系统包括源节点、目的地和中继节点，源节点给予中继节点奖励报酬，激励中继节点缓存文件、携带并转发文件数据，最终将数据传递到

目的地。

2.1 激励机制交易形式

在互联网中，激励机制大多通过使用电子货币作为激励方式来促使组织者、参与者协同工作、达成目标，激励机制的激励过程可以看做报酬的交易过程。基于区块链的激励机制可通过本身的密码学技术来为交易过程提供安全保障。区块链本身的交易模式能够防双花、防窜改，区块链技术通过盖时间戳并发布全网的方式，保证每笔货币被支付后，不能再用于其他支付；区块链上的信息一旦经过验证并添加至区块链后，就会得到永久存储，除非能够同时控制系统中超过51%的节点，否则单个节点上对数据库的修改都是无效的，从而保障了数据不被非法窜改。

然而激励机制除了考虑付款形式能够防双花、防窜改外，还需考虑交易效率、交易安全性、交易隐私问题。

激励机制的交易过程应降低延时，限时承诺机制可以保证交易付款的时效性。限时承诺机制通过时间上的限制和设定契约金的方式来确保有效性，当交易的合法性认定后需在规定的有效时间内进行交易付款。Andrychowicz 等人[19]基于比特币设计了一种“定时承诺”机制，必须在限定时间内完成任务，否则就会支付罚款，设计的具备定时承诺机制的交易 T_x 流程如图 1 所示。

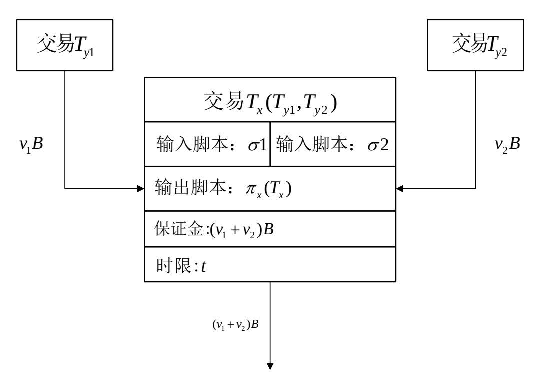


图 1 定时承诺机制

Fig. 1 Timing commitment mechanism

其中 T_{y1} 、 T_{y2} 作为前面交易的索引值， B 为交易时代表的比特币值， π_x 作为 T_x 交易的输出脚本，t 作为每个交易的时间锁，它表示只有在 t 内交易达成，该笔交易才具备有效性。定时承诺机制的承诺协议是在输出脚本当中进行描述的，承诺协议的描述由于设计者考虑不周而存在安全性问题。

交易过程中应要求有尽量少的信息传输、较低的管理和存储需求，即速度和效率比较高，而且交易中经常会有小额的货币支付交易产生。Poon 等人[20]提出使用微支付通道网络在具有长期合作两节点间进行可信交易，交易不公布在公有链上，仅记录微支付通道中两个节点的 bitcoin 总额。微支付网络减少了区块的大小，降低了矿工的计算工作量，提升了比特币的可伸缩性，实现近乎即时的交易效率，其设计的微支付通道网络模型如图 2 所示。

通道建立阶段，A 与 B 各自把 X 个 BTC 转给一个由两人共同控制的多签名地址，由此开通支付通道，该地址写入比特币网络；链下交易阶段，A 与 B 可在支付通道中进行不广播、不记录的链下交易，且零手续费；关闭通道阶段，在实现多比交易且无交易需求后，可由 A、B 关闭通道，通道关闭时发起交易并广播到主网，由矿工记录后完成。微支付通道的链下交易仅在局部节点中进行，难以保证安全性。

当密码货币作为激励机制时，由于没有对应的措施来限定节点的转账金额，节点可不按规定的定价策略来转账，而且矿工节点可能发起欺骗攻击、合谋攻击，造成了激励机制的不安全。可信硬件的方式需更换现有设备，成本代价较高；将承诺记录区块链的方式，可防止承诺被窜改，是相对可行的方式。Kumaresan 等人[21]提出了基于 Bitcoin 的功能转账模型，通过 Bitcoin 构造形式化的模型来支持限时转账、承诺退还、押金补偿等功能，并通过这些功能转账模型实现了可证计算、安全计算、公平计算、非交互赏金任务(Noninteractive bounties)等密码学任务。Matsumnoto 等人[22]提出一种基于区块链的公钥基础设施(PKI)认证中心(CA)安全激励机制，通过定义 CA 不诚实行为和制定奖惩措施来激励 CA 展现诚实行为，采用以太坊(Ethereum)智能合约保存 CA 注册信息、不诚实行为、奖惩交易和监管者的记录等信息，从而保证激励机制的安全可信。

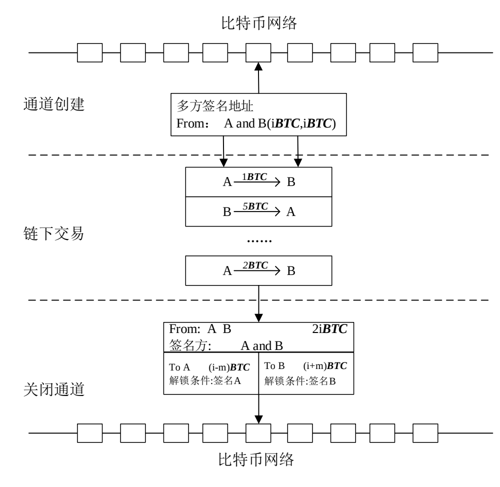


图 2 微支付通道网络模型

Fig. 2 Lightweight-Payment network model

交易过程应该保证不泄露信息，即使在如比特币网络中交易也会存在关联问题，通过交易记录信息和去匿名方法获取用户真实信息，如何提升交易关联度成为实现交易过程隐私保护的关键。Liu 等人[23]提出了一种不可链接的硬币混合方案，允许用户在不相信第三方的情况下混合他们的比特币。这种混合方案使用了一种环签名的原语，利用椭圆曲线数字签名算法(ECDSA)来隐藏地址间的硬币转移操作痕迹。上述方法与达氏币使用的混币(CoinJoin)技术相似，用户的交易通过随机选择多个主节点，并在这些节点中依次进行混合，最后输出。这样增加了攻击者猜测交易关联度的难度，除非攻击者控制了很多节点，否则几乎不可能对指定交易进行关联，从而保证了用户交易过程的隐私保护需求。Sasson 等人利用非交互式的零知识证明(zk-snark)构建了 zerocash 支付框架，实现了对支付目的地和金额的强隐私保护效果。

2.2 激励机制分类

基于密码货币的激励机制将密码货币作为激励机制的报酬，奖励达成任务目标的参与者。现有激励机制的分类包括内在激励和外在激励[24]，内在激励包括自我实现激励、娱乐激励等，外在激励包括物质激励和电子货币等。激励机制还被分为娱乐激励、服务激励、货币激励等方式[25~27]。在互联网中，电子货币常作为激励机制的报酬。定价策略用于确定报酬的金额，会影响激励机制的合理性与公平性，因此按定价策略将激励机制分为三类：

1) 基于信誉的激励机制

基于信誉的激励机制将信誉、信任量化，将其作为主要参数，依据不同条件下的因素，将各参数通过响应的计算方式，最终得出符合条件的报酬价格。该类定价策略依赖的信誉系统可分为集中式和分布式信誉系统。集中式信誉系统由中央机构记录、收集、发布用户的历史交易信息及信誉反馈信息，但其运行成本高，且存在中心信任缺失问题。分布式信誉系统将节点的信誉信息分散存储在交易过的节点上，查询时

广播查询信息，由交易过的节点响应并反馈对应的信誉值。

Wang 等人[28]针对移动用户中存在自私节点的问题，提出了基于信誉和信任的激励机制。该激励机制模型分为用户选择模块和奖励实施模块，通过三种元素的定价因子对服务提供者进行综合定价计算，抑制自私节点的自私行为。模型由服务请求者、服务平台和服务提供者三部分组成。在用户选择模块中平台通过服务提供者的信誉值和信任值，选择优胜者。在奖励执行模块中定价策略 P_j 由服务质量 Q 、链路强度 S_{link} 、服务提供者在有限时间内访问的概率 F_{zt} 综合计算：

$$P_j = l(\vartheta Q + \delta S_{link} + \zeta F_{zt}) \tag{1}$$

其中 l 作为任务的强度 ϑ,δ,ζ 是三个定价因子的权重且 $\vartheta+\delta+\varsigma=1$ 。通过这三个因素来表示转发质量的优劣，质量越高、价格越高。任务执行后，分别更新请求者和提供者的信誉值、信任值。Bogliolo 等人[29]提出了一种在特定环境下基于虚拟货币和基于信誉联合使用的激励方式，通过合作激励以避免自私的搭便车节点损害整个系统。该方式发现和请求、协商、交易、评估和反馈四个阶段，其中对任务的定价使用了基于信誉的分段线性函数：

$$C(T) = \begin{cases} C_{\min} + \dfrac{C_{\max} - C_{\min}}{T_{th}}(T_{th} - T) & T < T_{th} \\ C_{\min} & T > T_{th} \end{cases} \tag{2}$$

C 为信任成本，T 为请求方的信任值，$C_{\min}$ 是请求者在不考虑自身信誉的情况下要求的最小报酬(成本)，$C_{\max}$ 是请求为不受信任的用户提供的最大报酬，T_{th} 是在使用最小成本下的信誉阈值。

然而信誉量化的合理性很难被认可，如定价因子比例分配的合理性和阈值设定的合理性，同时也面临洗白攻击、女巫攻击等问题[30]。

2) 基于拍卖的激励机制

基于拍卖的激励机制将任务的分配方式以拍卖的形式执行，通过竞价使任务请求者和任务参与者利益最优化。基于拍卖的定价策略可分为 Myerson 拍卖、VCG 拍卖、双边拍卖、多属性拍卖机制、逆向拍卖。

在竞价机制中，卖家的核心问题是如何依据拍卖规则与买家的出价来获取最大化收益，在 1983 年 Myerson 提出了 Myerson 引理[31]用于解决上述竞价机制中出售单个物品的“最优拍卖问题”。当任务发起者发布了一个信息传输任务后，参与者与发布者在损失交易的一定效率情况下报出自己可以接受的真实报酬以达成交易。然而 Myerson 引理并不能解决多个物品出售情况下的最优问题。

在组合拍卖场景中，如何对多个商品分配出售达到最优收益成为关键挑战。VCG(Vickrey-Clark-Groves)机制解决了上述问题。 VCG 拍卖机制基于动态定价策略，其定价策略是依据竞价者对于其他竞价者造成的利益损失来定价的。如图 3 所示，在 VCG 机制下，竞价任务中第 m 个任务的定价由它在竞价中的排序结果来决定，对于第 n 个任务($n \le m$)的定价不受 m 的影响，当 $n > m$ 时，对于任务 m 的定价相当于 m 的存在对任务 m 的竞价排序之后的任务效益损失之和。VCG 拍卖机制是一种全局最优化策略，通过激励机制的设计和合理的支付函数引导参与节点诚实地上传自己的实际报价，提供更加稳定的交易环境。David 等人[32]分析了买方与卖方的非对称场景，提出了加权双边 VCG 拍卖机制，在不增加开销优化问题的复杂程度下，通过牺牲分配的最优性实现次优分配。Shajaiah 等人[33]基于 VCG 机制设计了一种能源交易拍卖机制，采用 Paillier 密码进行同态加密，确保了用户隐私的保护和竞价物品的价值，避免了拍卖商的不诚实行为。

基于双边拍卖机制激励结构,其中，平台(拍卖师)向移动用户(一方投标人)购买数据，并将数据出售给感知任务所有者(另一方的投标人)。在该拍卖中，首先，平台宣布分配规则(任务选择和用户调度)和支付规则(对被调度用户的支付价格和对所选取任务收取的价格)。然后，每个任务提交一个价值(出价)，并且每个用户向平台提交感知成本向量(出价)，其可以与真实任务值或成本向量不同。最后，平台根据所有任务和用户的出价以及其他公有信息计算分配和收付款。本文主要考虑设计真实的拍卖机制，其中，任务和用户将如实提交其私有信息。Yong 等人[34]设计了在蜂窝网络中多源用户和空闲用户间的双重拍卖机制，通过双边拍卖解决在能源缺少情况下，源用户向其他闲置用户购买中继服务的最优分配问题。

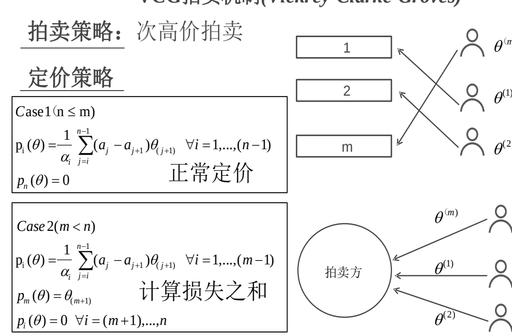


图 3　Vickrey-Clark-Groves 拍卖机制

Fig. 3　Vickrey-Clark-Groves auction mechanism

基于多属性拍卖机制与大多单一拍卖不同，这种拍卖竞争通常涉及许多价格以外的方面如性能、质量。平台对技术特征、交付日期、管理性能以及成本等信息通过复杂的评分系统判定后，将合同交付给总分最高的参与者。Che 等人[35]在政府采购竞标背景下，设计建立了基于质量和价格的二维投标模型，并使用了第一分、第二分和第二优先出价三种拍卖方案。该方案通过利用买方按照自身最大利益承诺的评分规则来实现最优结果。Kang 等人[36]研究了在数字产品拍卖场景下的在线逆向多属性拍卖机制，将多属性引入传统的在线逆向拍卖机制，实现在卖方不确定的情况下，买方最大化收益的策略。

基于逆向拍卖机制是指一种存有一位买方和许多潜在卖方的拍卖方式，买方发布任务需求，供应者在有效时间内通过专门的网络平台进行交互实时竞价，竞价结束时的报价为各个供应者的最终报价，最终通过综合评价模型来为买方确定优胜的供应者。Chen 等人[37]研究了在逆向拍卖中四个属性对供应商投标策略的影响，优化了买方与卖方信息不平等的问题。Zhang 等人[38]提出了一种二阶段逆向拍卖机制，通过挖掘隐含价格和质量属性间关系来获取最优组合，使供应商提供私人信息，买方通过信息获取高质量任务。

3) 基于质量贡献的激励机制

基于质量贡献的激励机制将任务分配给参与者，在任务完成后通过质量计算模型得出任务质量的代价等级，依据任务质量对参与者支付相应报酬。

Gao 等人[39]针对群智感知中的激励性不高的问题和贡献质量问题提出一种基于质量意识的激励机制，创建效用函数优化数据质量和设置额外报酬奖励，使任务报酬与贡献质量更加准确。被选中的参与者可获得报酬 $c'_m = c^b_m + c_m$ ，c_m 作为基础奖励， c^b_m 作为额外奖励。

Jin 等人[40]针对如何激励移动群智感知参与任务问题提出了一种基于参与人员信息质量的激励机制，通过质量指标获得低成本下高质量的数据，其定价函数：

$$u_i = \begin{cases} p_i - c_i, & \text{if } i \in S \\ 0, & otherwise \end{cases} \tag{3}$$

其中 p_i 作为任务报酬， c_i 作为参与人员的成本， u_i 作为参与

人员的工作效能，$i \in S$ 即任务优胜集合中的参与人员。

Yu 等人[41]针对群智感知数据质量差的问题，提出了一种基于信誉的激励机制，对参与者的感知数据质量进行信誉量化，并根据信誉值给与一定数额的虚拟优惠券，使得高质量贡献者在定价排名中优先。虚拟优惠券是对之前获取任务失败的参与者的补偿，增加参与者下一轮竞标的中标机会。参与者 i 在第 j 轮的虚拟优惠券定义为

$$d_{i,j}=\begin{cases}d_{i,j-1}+\gamma\cdot r_i, & i \text{ is a loser in } (j-1)\text{th auction},\\ 0, & i \text{ is a winner in } (j-1)\text{th auction}.\end{cases} \tag{4}$$

其中 $d_{i,j-1}$ 为参与者 i 在第 j 轮的虚拟优惠券，γ 表示虚拟优惠券的数量，r_i 表示参与者 i 的信誉量化值。该虚拟优惠券用于提升定价排名，增加获胜可能性。定价排名定义为

$$rp_i=b_i-d_i \tag{5}$$

其中 b_i 表示参与者 i 实际竞价，d_i 表示参与者 i 使用的虚拟优惠券，每轮拍卖选择定价排名较高的参与者作为获胜者。

基于质量贡献的激励机制受限于质量能被量化的场景，也存在对低质量参与者不友好、任务参与者参与度不高等问题。

3 激励机制评价标准

激励机制评价标准是用于衡量基于场景和支付方式下的激励机制的安全性、隐私保护、性能等的手段，主要包括 a)安全可信，旨在解决激励机制中的自私节点问题以及矿工为了利益最大化发动假冒攻击、联合参与节点发动合谋攻击情景；b)隐私保护，在激励机制的设计中考虑节点信息的隐私保护；c)可拓展性，解决基于密码货币的激励机制中的交易瓶颈问题；d)成本开销，考虑实现激励机制所需要花费的开销问题；e)可持续性，考虑如何可持续性地保持用户参与性问题。

3.1 安全可信

激励机制中存在着自私节点因为自身利益最大化而在交易中展现非法行为的问题。安全可信是指采取相对应的措施保证用户交易安全且互相可信任。防止非法行为采取的策略通常是使用身份认证机制，在交易过程中通过签名来提供节点行为的有效证明。He 等人[42]构建博弈模型来分析激励机制的安全性。针对分布式应用机会传输中的节点的安全可信问题，构建报酬定价博弈模型，其建立的不同定价策略下的参与者最优响应策略略为

$$p_i=\begin{cases}\alpha/2^{n-1}, & \text{if } i\in P,\\ \beta, & \text{if } i\in E,\\ 0, & \text{otherwise}\end{cases} \quad and \quad \begin{cases}\alpha>2^{n-1}c_{\max},\\ \beta>c_E,\\ \alpha<\beta/q^2.\end{cases} \tag{6}$$

其中，p_i 为节点 i 的最终支付报酬，α,β 为报酬相关参数，P 为中间节点集合，E 为接收者，c_E 是接收者的通信代价，$c_{\max}$ 是中间节点的最大通信代价，q 为两个节点的相遇概率。作者还通过形式化证明了在 $\alpha>2^{n-1}c_i$ 和 $\beta>c_E$ 条件下能够抵抗中间节点或矿工节点的欺骗攻击，在 $\alpha>2^{n-1}c_i$ 条件下能够抵抗接收者与矿工节点的合谋攻击，在 $\alpha>\beta/q^2$，$\alpha>2^{n-1}c_i$ 条件下能够抵抗中间节点与矿工节点的合谋攻击。如图 4 所示，在给定相关参数量的情况下，可以实现当中间节点跳数不超过 5 时，抵抗以上所述的欺骗攻击和合谋攻击。

通过使用密码学技术本身的安全性，从而达到激励机制的安全可信。比如 Li 等人[1]对交通路况系统进行了分析，提出了基于信誉的激励机制用于激励用户分享交通实时信息，利用环签名、椭圆曲线等密码学技术解决声明过程中的自私节点、欺诈攻击问题等。Cheng 等人[43]提出了一种基于延迟转发网络的安全激励机制，通过使用签名和验签技术激励中间节点的转发行为，解决了自私节点问题。

门限签名作为密码学技术可被用于解决安全可信当中的抗合谋攻击问题。门限签名是指一个任务由 n 个成员共享群体密钥，当参与签名的成员数目大于或者等于规定的门限值 t 时，就能代表群体产生签名，任何验证者都可以用群公钥验证签名的有效性。其安全性规约为计算 Diffie-Hellman 难题——如果不存在一个概率多项式的算法 A 在时间 t 内以至少 ε 的概率解决循环群上 CDH 问题，那么 $(t,\varepsilon)-$CDH 问题假定成立，那么门限签名方案是安全的。2006 年 Yang 等人[44]提出了基于模糊身份的签名方案。2007 年由 Khader[45, 46]提出了基于属性的群签名方案和具有匿名撤销功能的基于属性群签名方案。Chen 等人[47]分析了现有的基于属性门限签名方案，利用引入秘密随机因子防止合谋攻击者利用组合私钥的方式伪造签名。Qin 等人[48]提出了一种基于访问结构的安全身份阈值签名方案，降低了基于拉格朗日插值的(t，n)阈值结构的设计复杂性，使系统应用范围更管，提供了自适应选择消息攻击下的安全证明，确保系统安全可信。

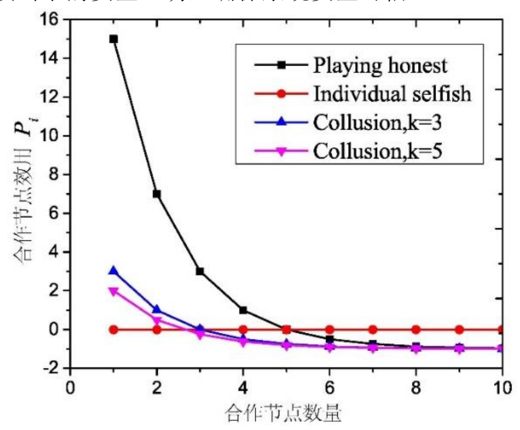


图 4 不同中间节点跳数下的节点效用

Fig. 4 Utility of different cooperative nodes

3.2 隐私保护

激励机制设计还应考虑不泄露个人隐私信息，但区块链的公开性常常会造成用户之间的激励关系、用户身份或用户行为被泄露。Wang 等人[10]通过 K 匿名方法达到激励机制的隐私保护。针对基于区块链的加密货币作为激励方式，矿工负责量化和验证感知质量获取节点隐私的问题，k 匿名方式将部分验证工作分担给任务中的节点以保护隐私。单一节点完成验证工作会较高程度增加存储、计算、通信开销，易于通过 IP 地址被追踪，节点组协作方式在交易验证中更加高效。如图 5 所示，在验证过程中系统将矿工的一部分工作分配给节点组，服务器 S 与用户组 G 进行交易，一个组 G 由 k 个用户组成，用户通过节点组对隐私数据脱敏，使得攻击者对于组内任意一条数据记录进行攻击时关联到组内 k-1 条记录，导致无法确定关联信息，减少了链接攻击所带来的隐私风险。

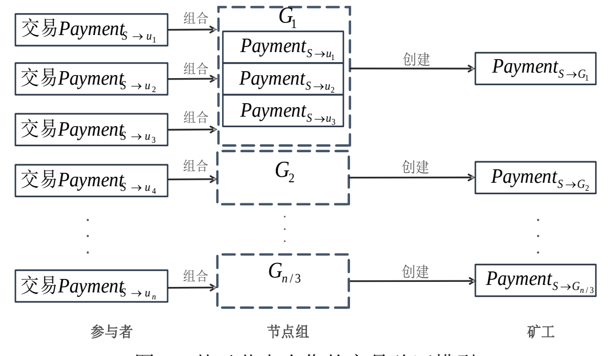


图 5 基于节点合作的交易验证模型

Fig. 5 Transaction verification model based on node cooperation

Kim[49]提出了一种按需分配的激励方式，利用群体签名技术保护用户的位置和隐私。Zhuo[50]提出了一种用于众包隐私保护的框架，使用差分隐私技术保护了矿工的数据隐私。

3.3 可拓展性

可拓展性是指保证信息网络服务质量和效率,在不牺牲安全可信、隐私保护、通信开销等情况下达到系统的可伸缩性、高效率等。激励机制需要考虑矿工验证效率问题、交易效率问题、基于密码货币的激励机制在众包、DTN 网络等动态网络中出现的交易瓶颈问题等。比如 Luu 等人[51]提出了一种可扩展的公有链分布式共识协议，该协议将系统中的节点随机划分为组，并行验证不同交易，通过拜占庭协议来达成组内共识，以达到增强交易的吞吐量，使得计算能力对单位时间的交易数量几乎达到线性增长，然而组内采用采用的拜占庭协议时延较大。图 6 展示了基于拜占庭协议的网络延迟情况，可以看到，即使拜占庭网络规模在 100 时，其延迟也会随着网络规模呈现二次方增长，而且但有恶意节点存在时，其延时将会继续上升。

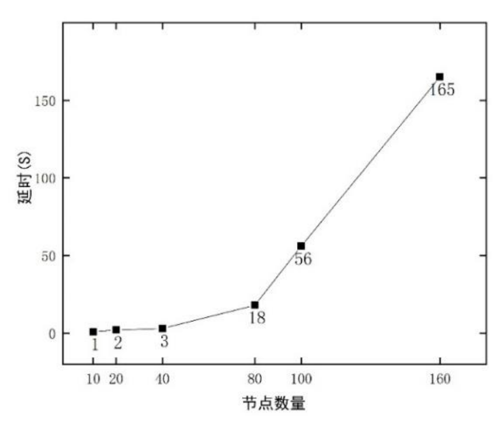


图 6　基于拜占庭协议的网络时延情况

Fig. 6　Network delay based on Byzantine failures

Bitcoin-NG[52]是一种基于比特币信任模型的可拓展区块链协议，通过将传统的比特币挖矿分为关键块(keyblocks)和微块(microblocks)两种模式。关键块用于首领(leader)选举，保持着传统区块十分钟的时间间隔，保证了安全性。微块用于记录交易，不包含工作量证明，出块时间 10 秒，提升了交易速度。Bitcoin-NG 作为一个序列化交易的区块链协议，在不牺牲其他条件的情况下优化了延迟和带宽。图 7 显示了不同数量微块下 Bitcoin-NG 的延迟，随着网络节点数量增多、组内块数增多，系统的性能会降低，而 Bitcoin-NG 协议中节点必须向整个网络广播所有块，因为这是协议中序列化交易所必需的一步，因此随着网络扩展，块吞吐量的增加需要更长的延迟。

Sompolinsky 等人[53]在 bitcoin 原有协议的基础上进行了改进，使用 DAG 图结构代替块链结构，优化了交易处理的等待时间，并在保证安全性前提下增加了处理交易的速率，将块生成速率提高到之前的 600 倍。

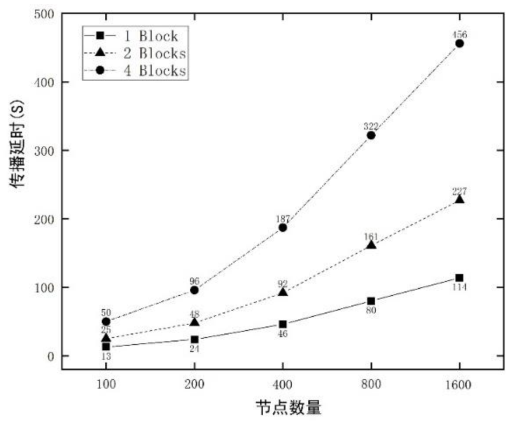


图 7　Bitcoin-NG 网络时延情况

Fig. 7　The network latency of bitcoin-NG

4　结束语

本文调研并回顾了目前较新的有关区块链技术的激励机制研究。首先概述了区块链的概念，对比分析了密码货币的属性；然后从基于区块链的激励机制分析激励机制的交易方式，依据激励机制中的定价策略对激励机制进行了分类分析，以及总结基于区块链的激励机制的评价标准如安全可信、隐私保护、可拓展性等，总结并讨论了激励机制在区块链技术下的优势、劣势。文献综述表明：在基于区块链下的激励机制研究还处于起步阶段，未来仍需针对基于区块链的激励机制的需求和目标加以改进，应更多地探索结合激励机制与区块链的优势当在具体设计激励机制时，区块链激励架构还无法做到精确适配，一些策略的细节也未能详尽，未来的基于区块链的激励机制还需在以下几个方面展开研究：

a) 相关激励策略的兼容适配问题，不同密码货币、定价策略及支付形式对硬件性能、系统等都有相应的要求，是否能够在相应的应用场景下实施或改进适用是值得研究的问题。例如在物联网应用场景中如何使用轻量级密码货币进行物联网设备的激励，如何将具有隐私保护属性的货币应用于云计算的相关场景中，保证数据的安全性，如何利用定价策略实现大数据平台交易的公平性、可信性。

b) 激励效果性能提升问题，区块链作为一项新兴技术在隐私保护、可扩展性等方面还有很多需要优化的问题，还需要在某些激励效果方面做到质的突破，例如通过零知识证明技术来增强隐私保护的效果，在此基础上实现加密搜索、访问控制等，利用并行处理技术、批处理、批认证技术等 增强交易验证速度，提高激励机制的可拓展性。

c) 多目标联合优化问题，激励机制实际应用时往往更为复杂，需联合考虑多种激励效果进行优化，而且有些激励效果之间是相互冲突的，如隐私保护与效率、安全可信与可用性、成本开销与安全性。

d) 与中心化激励机制有机融合，中心化激励机制目前已广泛存在，完全替换现有中心化激励机制可能不太现实，如何让基于区块链的激励机制与中心化激励机制共存、有机融合是亟待要解决的问题。

参考文献：

[1] Li L, Liu J, Cheng L, Qiu S, Wang W. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19 (7): 2204-2220.

[2] Zhang Y Q, Bai X Y, Liu Q. Incentive mechanisms in mobile delay tolerant network [C]// 2017 7th IEEE International Conference on Electronics Information and Emergency Communication, 2017: 184-188.

[3] Yang C G, Xiao J, Li J D, Shao X Q, Anpalagan A, Ni Q, Guizani M. DISCO: Interference-Aware Distributed Cooperation with Incentive Mechanism for 5G Heterogeneous Ultra-Dense Networks [J]. IEEE Communications Magazine, 2018, 56 (7): 198-204.

[4] Zhan Y, Xia Y, Zhang J, Wang Y. Incentive Mechanism Design in Mobile Opportunistic Data Collection With Time Sensitivity [J]. IEEE Internet of Things Journal, 2018, 5 (1): 246-256.

[5] Islam M A, Mahmud H, Ren S, Wang X. A Carbon-Aware Incentive Mechanism for Greening Colocation Data Centers [C]// IEEE Transactions on Cloud Computing, 2017: 1-17.

[6] Zhai Y, Bai X, Liu Q. Incentive mechanisms in mobile delay tolerant network [C]// IEEE International Conference on Electronics Information & Emergency Communication, 2017: 184-188.

[7] Rezai A A, Torki L. The impact of the electronic money development in

the profitability of DBS banks of Singapore [C]// International Conference on E-commerce in Developing Countries: with Focus on E-trust, 2014: 1-9.
[8] Huicong Security Network. The top ten data breaches in 2017, [OL]. [2018-10-01]
[9] Sohu News Website. Sohu, The top ten data breaches in 2016, [OL]. [2018-10-01] http://www. sohu. com/a/122021640_526642
[10] Wang J Z, Li M R, He Y H, Li H, Xiao K. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications [J]. IEEE Access, 2018, 6 (3): 17545-17556
[11] Kuzuno H, Karam C. Blockchain explorer: An analytical process and investigation environment for bitcoin [C]// Electronic Crime Research, 2017: 9-16.
[12] Urien P. Towards secure Bitcoin fast trading: Designing secure elements for digital currency [C]// International Conference on Mobile & Secure Services, 2017: 1-5.
[13] Neudecker T, Andelfinger P, Hartenstein H. Timing Analysis for Inferring the Topology of the Bitcoin Peer-to-Peer Network [C]// Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People, & Smart World Congress, 2017.
[14] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, [OL]. [2018-10-01] http://www. bitcoin. org/bitcoins. pdf
[15] Gobel J, Krzesinski A E. Increased block size and Bitcoin blockchain dynamics [C]// Telecommunication Networks & Applications Conference, 2017: 1-6.
[16] Li L, Liu J, Cheng L, Qiu S, Wang W. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2018, PP (99): 1-17.
[17] Sheshjavani A G, Akbari B, Ghaeini H R. A free-riding resiliency incentive mechanism for VoD streaming over hybrid CDN-P2P networks [C]// International Symposium on Telecommunications, 2017: 771-776.
[18] Ezzahidi S A, Sabir E, Kamili M E, Bouyakhf E H. A non-cooperative file caching for delay tolerant networks: A reward-based incentive mechanism [C]// Wireless Communications & Networking Conference, 2016.
[19] Andrychowicz M, Dziembowski S, Malinowski D, Mazurek L. Secure Multiparty Computations on Bitcoin [C]// IEEE Symposium on Security and Privacy, 2014: 443-458.
[20] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments [OL]. [2018-10-01] http://lighting: network-network-paper: pdf, 2016
[21] Kumaresan R, Iddo B. How to Use Bitcoin to Incentivize Correct Computations [C]// 21st ACM Conference on Computer and Communications Security (CCS 2014) , November 3-7, 2014.
[22] Stephanos Matsumoto, and Raphael M. Reischuk. IKP: Turning a PKI Around with Decentralized Automated Incentives [C]// The 38th IEEE Symposium on Security and Privacy (S&P 2017) , May 22-24, 2017, San Jose, CA, USA
[23] Liu Y, Liu X T, Tang C J, Wang J, Zhang L. Unlinkable Coin Mixing Scheme For Transaction Privacy Enhancement of Bitcoin [J]. IEEE Early Access Articles, 2018, 6 (4): 23261-23270
[24] 王娟，王丽清，马文倩，徐永跃. 群智协同激励机制研究综述 [J]. 计算机工程与应用, 2020: 1-12
[25] Jaimes Luis G, Vergara-Laurens Idalides J, Raij Andrew. A Survey of Incentive Techniques for Mobile Crowd Sensing [J]. IEEE INTERNET OF THINGS JOURNAL, 2015 (2): 370-380
[26] Hui Gao, Chi Harold Liu, Wendong Wang, Jiaxin Zhao, Zheng Song, Xin Su. A Survey of Incentive Mechanisms for Participatory Sensing [C]// IEEE Communications Surveys & Tutorials, 2015, 17 (2): 918-943
[27] Xinglin Zhang, Zheng Yang, Wei Sun, Yunhao Liu, Shaohua Tang, Kai Xing, Xufei Mao, Incentives for Mobile Crowd Sensing: A Survey [C]// IEEE Communications Surveys & Tutorials, 2016, 18 (1): 54-67
[28] Huilin Wang, Chunxiao Liu, Yanfeng Wang, Dawei Sun. A Novel Incentive Mechanism Based on Reputation and Trust for Mobile Crowd Sensing Network [C]// 5th International Conference on Cross-Cultural Decision Making, 2016.
[29] A Bogliolo, P. Polidori, A Aldini, Virtual Currency and Reputation-Based Cooperation Incentives in User-Centric Networks [C]// 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC) , Aug. 2012.
[30] Xuewen Dong; Qiao Kang; Yang Xu; Zhuo Ma, Teng Li. Poster Abstract: A Practical Sybil-Proof Incentive Mechanism for Multichannel Allocation [C]// IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) , 2019
[31] Myerson R, MA Satterthwaite. Effient mechanism for bilateral trading [J]. Journal of Economic Theory, 1983, 29 (2): 265-281
[32] David E, Azoulay R. It Does Matter Who I sell to and Whom I Buy From: Weighted Bilateral VCG [C]// IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2015: 126-129.
[33] Shajaiah H, Abdelhadi A. Clancy C. Secure power scheduling auction for smart grids using homomorphic encryption [C]// IEEE International Conference on Big Data, 2017: 4507-4512.
[34] Wang Yong, Yun Li, Liao Chao, Chong gang Wang, Xiaolong Yang. Double-Auction-Based Optimal User Assignment for Multisource–Multirelay Cellular Networks [J]. IEEE Transactions on Vehicular Technology, 2015, 64 (6): 2627-2636.
[35] Yeon-Koo Che. Design competition through multidimensional auctions [J]. The Rand Journal of Economics, 1993, 24 (4): 668-680
[36] Wanglin Kang, Lei Wang, Yanan Jiang. A Multi-attribute Auction Model for Online Digital Goods [C]// Proceedings of the 25th China control and decision-making conference, 2013.
[37] Chen Guowei. Reverse auction format choice decision based on supplier attributes [C]// International Conference on Service Systems & Service Management, 2015.
[38] Lufang Zhang. Reverse Auction Mechanism Design with Quality Preference [C]// International Conference on Service Systems & Service Management, 2015.
[39] Gao, Hui, Liu, Chi Harold, Tang, Jian. Online Quality-Aware Incentive Mechanism for Mobile Crowd Sensing with Extra Bonus [C]// IEEE Transactions on Mobile Computing, 2018.
[40] Haiming Jin, Lu Su, Danyang Chen, Hongpeng Guo, Klara Nahrstedt, Jinhui Xu. Thanos: Incentive Mechanism with Quality Awareness for Mobile Crowd Sensing [J]. IEEE Transactions on Mobile Computing, 2018, 18 (8): 1951-1964
[41] Ruiyun Yu, Jiannong Cao, Rui Liu, Wenyu Gao, Xingwei Wang, Junbin Liang. Participant Incentive Mechanism Toward Quality-Oriented Sensing: Understanding and Application [C]// Transactions on Sensor Networks 15 (2): 1-25.
[42] He Y H, Li H, Cheng X Z, Liu Y, Yang C, Sun L. A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications [C]// IEEE Access, 2018: 1-11.
[43] Cheng Gong; Wang Bo; Zhao Faru, SIS: Secure Incentive Scheme for Delay Tolerant Networks [C]// 2012 11th International Symposium on

Distributed Computing and Applications to Business, Engineering & Science, 2012

[44] Yang P, Cao Z, Dong X. Fuzzy identity based signature with applications to biometric authentication [J]. Compute and Electrical Engineering, 2011, 37 (4): 532-540.

[45] KHADER D. Attrebute based group signatures [OL]. [2018-10-02]. https://eprint. iacr. org/2007/159. pdf

[46] KHADER D. Attribute based group signature with revocation [OL]. [2018-10-01]. http://eprint. iacr. org/2007/241

[47] 陈桢，张文芳，王小敏. 基于属性的抗合谋攻击可变门限环签名方案 [J]. 通信学报, 2015, 36 (12): 212-222

[48] Qin H W, Zhu X H, Dai Y W. Provably Secure Identity-Based Threshold Decryption on Access Structure [C]// Tenth International Conference on Computational Intelligence & Security, 2014: 464-468.

[49] Kim M. Incentive mechanism with privacy-preservation on intelligent parking system utilizing mobile crowdsourcing [C]// 2017 4th International Conference on Computer Applications and Information Processing Technology, 2017: 1-4.

[50] Zhuo G Q. Privacy-preserving and fine-grained data aggregation framework for crowdsourcing [C]// Tenth International Conference on Mobile Computing and Ubiquitous Network, 2017: 1-6.

[51] Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S. A Secure Sharding Protocol For Open Blockchains [C]// Acm Sigsac Conference on Computer & Communications Security, 2016: 17-30.

[52] Eyal I, Gencer A E, Sirer E G, *et al.* Bitcoin-ng: A scalable blockchain protocol [C]// 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16) . USENIX Association, 2016: 45-59.

[53] Sompolinsky Y, Zohar A. Accelerating bitcoin’s transaction processing fast money grows on trees, not chain [OL]. [2018-11-01]. https://eprint. iacr. org/2013/881. pd